Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2016 International Conference on Human Factors in Cybersecurity, July 27-31, 2016, Walt Disney World, Florida, USA, Part III, pp. 169-182
DOI:10.1007/978-3-319-41932-9_14

# Human Capability Evaluation Approach for Cyber Security in Critical Industrial Infrastructure

**Uchenna P. Daniel Ani, Hongmei Mary He and Ashutosh Tiwari**

**Abstract** Every organization is as frail as its frailest human link in the cyber security of Industry Control System (ICS), which is without predisposition to conceivable technological solutions for enforcing security. Noticeably, human-involved systems are becoming more chaotic, and gravely under attacks due to irregular actions or inactions of human entities in the constituent chain. Many industrial cyber-attacks have successfully defeated technological security solutions through preying on human weaknesses in knowledge and skills, and manipulating insiders within organizations into unsuspectingly delivering entry and access to sensitive industrial assets. In order to help enterprises assess the level of employees' cyber security awareness and responsiveness, and enhance ICS Cyber security knowledge and skills for ICS protection, a Workforce Cyber Security Capability evaluation model is presented, and theoretically validated. A capability evaluation will allow industries to have a better understanding of the potential state of consciousness, readiness and diagnostic abilities of the industries; thus improve the prevention, detection, and response to any cyber-specific incidents.

**Keywords** Workforce-centred evaluation · Workforce security evaluation · Industrial security evaluation · Cyber security evaluation · Human-centred vulnerabilities

U.P. Daniel Ani (✉) · H.M. He (✉) · A. Tiwari (✉)
School of Aerospace, Transport, and Manufacturing. Manufacturing Informatics Centre, Cranfield University, Bedford, UK
e-mail: u.p.ani@cranfield.ac.uk

H.M. He
e-mail: h.he@cranfield.ac.uk

A. Tiwari
e-mail: a.tiwari@cranfield.ac.uk



D. Nicholson (ed.), *Advances in Human Factors in Cybersecurity*,
Advances in Intelligent Systems and Computing 501,
DOI 10.1007/978-3-319-41932-9_14

## 1 Introduction

While IoT technologies are bringing exciting benefits to Industry in real-time data and process management, it also yields a remarkable increase in cyber threats, vulnerabilities and risks. Large organizations, corporations, industries and businesses are continually investing huge in the development of technologies to protect their control system infrastructure (information, services and networks). However, the technical outcomes in Cyber security need the endorsement of the workforce in an organization. If the workforce do not understand and/or play their roles in the security design of the organisation. Cyber security assurance for industrial control systems (ICSs) and networks goes beyond the institution of antivirus, firewalls, and intrusion detection/prevention systems (ID/PS), etc. Even with updated technologies, stern security procedures, and high skilled IT security experts; it is still possible that an organisation would yet be unable to attain desired security without the improvement of security awareness of employees in the whole organisation.

Essentially, Cyber security is described as technologies and processes that are developed to protect computers, their hardware and software, networks and data [1], from unlawful access to the Internet by cyber criminals, hackers and terrorists [2]. In this work, Cyber security is defined as the '*harmonisation of capabilities in people, processes, and technologies; to secure and control both authorised and/or unlawful access, disruption, or destruction of electronic computing systems (hardware, software, and networks), the data and information they hold*. This definition stems from a perceptual view of the classic composition of a typical electronic system; comprising of three key collaborating entities: People, Process and Technology [3]—Fig. 1. The triad is considered prime to the '*success*' of every value provisioning digital system [4]. Here, *success* implies effective cyber-secure operations that guarantee pre-set system objectives. Figure 1 shows the intersecting results of employing security solutions that capture all 3 elements. The widening of this intersection implies greater Cyber security efficiency and assurance

Conversely, most current improvement efforts tend to focus on singular entities, flouting the others. Most information security solutions tend to focus more on technology strategies; discounting the people and process aspects [5]. Consequently, whatever enhancement initiative(s) targeted do not usually get achieved optimally

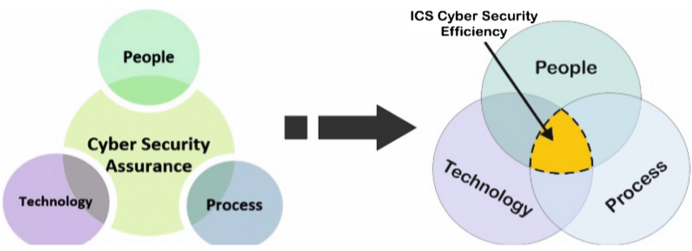


**Fig. 1** System-collaborative entities for effective cyber security

and durably due to the prejudiced approached adopted. This work focuses on the *'People'* aspect; characterising issues of communications, knowledge, skillsets, behaviour, and relationships that define the human elements of an industrial critical infrastructure [3].

## *1.1 Workforce-Related Cyber Security Issues*

Numerous high-tech progressions in Cyber security for information technology (IT), and operational technologies (OT) have enabled innovative monitoring and detection of threats, vulnerabilities, and attacks. Even with the potentials and doles of automation, the analytical competences of the human decision maker, through exploitation of cognitive processes, are still exigent and indispensable [6–8]. Users usually need to interact with *technologies* to manage system *processes* for better results. Nevertheless, human fallibility in the interaction loop makes and amplifies the tendency for slip-ups, and by-passing of existing security measures [9]. Hence, in spite of the massive deployment of technology solutions to protect ICSs, human factors still play a very significant role towards the implementation of desirable cyber-secure ICS environment. Thus, effective solutions must also be engaged by humans. While efforts continue to fortifying the technology piece of the large puzzle, intelligent attack gazers have turned to the weak pieces, especially; the people piece. Both amateurs and professional hackers now target people [9]. Potentially, the key security asset of an organization is often neither security technologies, nor laws and regulations, but the workforce—the *'people'* constituent [10]. Thus, the security of industrial infrastructure and services through manifold investments in money and time could be completely undermined, if this sector (employees or users) fail to understand and uphold its roles in the security solution of an organisation. An organisation is potentially as weak as its weakest workforce in the operational chain [10–12], and most successful attacks have exploited these shortcomings for their gain. These weak-links typically consist of expert control and automation engineers, technicians, and corporate service personnel [9, 13], who often ignore the importance of Cyber security, and are not keen to learn the knowledge and skills in Cyber security.

Records show that cyber-attacks are truly on the upsurge, with human entities being the most targeted vectors for malicious cyber actors. 36 % of the vilest security breaches in 2013 were caused by human errors from PWC's security breach report [14]. 31 % of dreadful security breaches in 2015 were initiated by human errors, and a further 20 % by purposeful misuses of systems still demonstrating a character trait of users [9]. 80 % of the time, stolen credentials through phishing are the root cause of data breaches [15]. While emphasizing the usability of security technology as an '*equivalent goal to the technology of security*' [16], people are noted to be the frailest link in the security chain. Therefore, the human within the ICS constituent chain pose a potential weak-link with high attraction to emerging cyber threats and attacks.

A human-involved approach is necessary to consolidate security levels within the ICS domain. Awareness of cyber vulnerabilities can be increased through the evaluation of the state of security awareness, and diagnostic abilities of the manufacturing workforce to expect, spot and react to cyber-specific incidents within the normal operational environment. Such evaluation could help to determine and understand the workforce's response aptitude to cyber-attacks. This leans on building/enhancement of security capabilities (knowledge awareness and diagnostic skills) of the workforce in ICS domain, which will obviously moderate the jobs of IT-Security experts/group to response, repairs and or recovery. The assessment of knowledge, and skills employs a proactive approach that would guide towards amplifying the workforces' security posture, and building better capabilities into the workforce; for self-protection, preservation of organisational work, and a conscious and cultured cyber-secure behaviour [10].

This discourse explores the potentials for understanding the aptitude of the *'people'* constituent to supplement the overall efforts of attaining a cyber-secure industrial environment. It is hypothesised that understanding the levels of knowledge, skills, and capabilities of the workforce of an organisation is key to grasping the overall organisation's Cyber security capability and susceptibility, and developing a high-skilled cyber workforce. Hence, a quantifiable and scalable approach for evaluating workforce cyber security capabilities (knowledge and diagnostic skills) will provide a reference to the organisation security level. The remaining part of this paper is outlined as follows; Sect. 2 reviews related work on cyber security capability evaluation with respect to human factors. Section 3 presents the proposed Workforce Cyber security Capability (WCSC) evaluation model, Sect. 4 presents the concepts and results of the theoretical validation of the WCSC model, and Sect. 5 presents the conclusions and future work.

## 2 Related Works in Cyber Security Capability Evaluation

Usually, an industrial organisation has a small team of IT experts, who manage its IT systems and services. A greater proportion of the employees; typically operational technology (OT) skilled use these IT systems and services for routine tasks. The improper use or abuse of these IT systems poses severe security risks to the overall industrial system. Security risks, which could result from weak passwords configuration, improper use of personal mobile devices, unprotected web access, inappropriate recognition and response to social engineering attacks, and several other anomalies. Most members of these workforce are often unaware of these security threats, hence, their actions could increase the risk of network intrusions, viruses, worms and trojan infections, loss of service response and productivity, and loss of proprietary and (or) confidential business/organization's information [10]. An essential step in the security scheme of organizations towards eliminating such vulnerabilities caused by its workforce is to have an overall Cyber security

assessment of its workforce. So that organisations could take corresponding steps to improve capabilities gaps through training or practice.

Capability has been prescribed as the product of knowledge, skills, and tools [17]. Although tools does describe capability on a generic context, it does not directly indicate people use proficiencies. Only knowledge and skills do. However, tools, as technology; may represent the attribute of an large organisation to cyber security [5]. In fact, the attitude of an organisation on Cyber security often also lie in the knowledge and skills that its workforce has. Knowledge and skills have the valued characteristics that represent WCSC. Tools as a factor is not considered in the proposed WCSC model because the model focuses on capturing direct human proficiencies alone. Tools only factors in when considerations are made for determine overall organizational Cyber security posture. Accordingly, the WCSC model would be a function of the security knowledge and skills of employees in an organisation. An evaluation model could help represent the workforces' security posture; build better capabilities for self-protection, work preservation, and culture Cyber security-conscious behaviour [10].

An International Telecommunication Union ITU survey reported 54 out of the 62 respondents identified with the importance of Cyber security awareness in achieving secure cyberspace [18]. Security '*awareness*' is simply meant to emphasis thoughtfulness on security, enabling individuals (workforce—employees and managers) to recognise security concerns and respond accordingly [19].

A study also indicated that supplementary knowledge of Cyber security can facilitate the spot-on detection of malicious cyber events and reduce the false classification of non-threatening cyber events as malicious [8]. Thus, skills can guide users to make right decisions and actions capable of reducing or eliminating the occurrence of malicious events. The assessment of cyber security capability is quite instrumental towards achieving an efficient workforce security consciousness [10]. This could be done through different approaches, such as *interviews (structured and semi-structured)* [20], *questionnaires* [21], *observations and gamifications* [8, 22], *penetrations testing* [23], etc. Although, several methods have emerged for evaluating workforce features and capabilities in the context of cyber security, we have not found any research that has offered a scheme of discrete numerical model to represent a status of an individual or the entire organisation in adhering to defined or expected cyber security policies and/or standards.

## 3 The WCSC Evaluation Model

Reaching Cyber security assurance for ICS is partly dependent on the efficiency and responsiveness of the workforce, which could produce a projection of organisational Cyber security capability, and guide human's behaviour as expected. ICS workforce can be roughly categorised to 3 parties; (i) IT security experts, (ii) Engineers/Field Operators/Technicians, and (iii) Corporate Managers. For the latter two, their behavioural activities often affect overall system security.

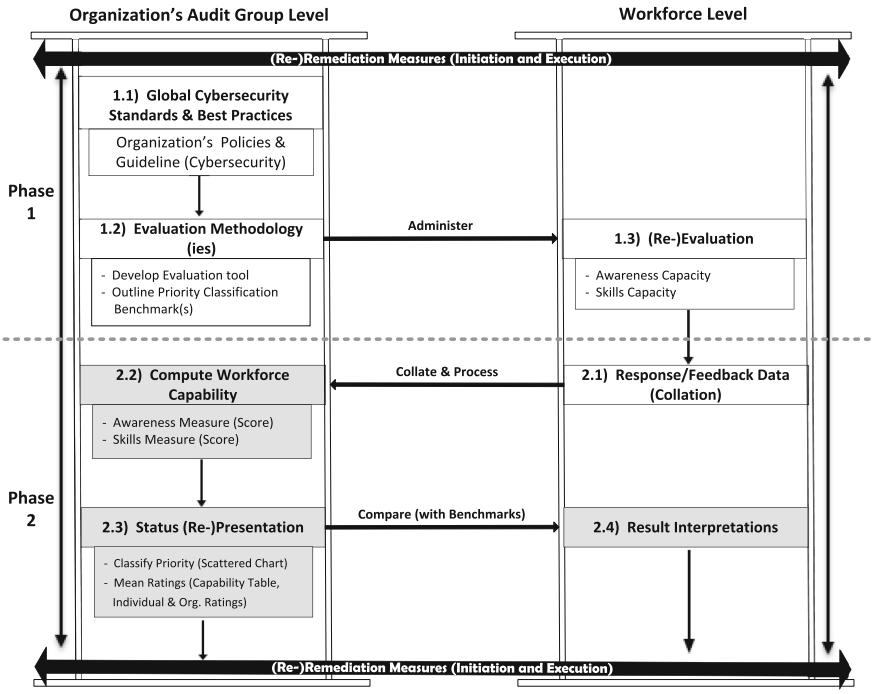


**Fig. 2** Workforce cyber security capability evaluation model

WCSC is represented as a function of knowledge, and skills levels. Here, knowledge level is defined as *the measure of information and theoretical understanding about recurrent cyber threats, vulnerabilities, attack patterns and impacts to the target system that a user, employee or operator is working with.* Skill level is defined as *the ability to use accumulated knowledge either from experience or training to spot or detect cyber-attack attempts, patterns and techniques, and the degree, in which the user can respond timely with appropriate countermeasures.* While the knowledge level implies the consciousness to potential Cyber security threats and possible economical loss from any unintentional or intentional errors, the skill level builds a technical muscle into people to efficiently and appropriately identify those threats, such that the damages and/or economical losses could be avoided or mitigated. Essentially, WCSC evaluation needs to cover information gathering, concerning the adherence to current/adopted security standards and policies, operational processes, cyber security trends knowledge and skill gaps in individual persons [24].

Figure 2 describes the process-flow of the WCSC Evaluation (WCSCE) model. It begins with defining ICS cyber security requirements relative to the functional objectives of a host organisation, the adoption of suiting evaluation methodology,

tools, capability priority classifications, execution of the evaluation, and (re)presentation of results. The process is divided into two broad stages; (1)—*Capability outline*; which involves the development of capability requirements, attributes, and their applications, (2)—*Analysis and Representation;* i.e., the examinations of results and interpretations for informed decision. The key contribution of this paper is captured in the grey shaded section (sub-stage 2.2) of the process flow; where a computational approach is proposed for evaluating the WCSC, and susceptibility classification of ICS workforce in an organisation. This capability evaluation model could be employed as a means of initial assessment (*first time evaluation after a typical system setup*), or for subsequent re-assessment (*where capability gaps and remediation will be investigated from initial assessment*). In the latter case, the process model becomes valuable for determining the new state of the workforce, and can provide a reference for creating remediation strategies.

## *3.1 Global Standards and Best Practices (Cyber Security)*

The process of evaluating WCSC begins from a foundational stage of specifying basic system/operational cyber security requirements. From the pool of existing security publications, it is suggested that organisations should follow national and international standards in Cyber security, and build the specific objectives and strategies based on their unique operational scenarios. Due to the variability of ICSs, their does not exist one security standard that completely covers all ICS domain. A blend of ICS-oriented security provisions, such as UK Cyber security Strategy, ISO/IEC 27000 series, NIST SP800 16, 18, 82 series, US DIACAP 8510.01, FIPS 199, 200, 201-2, etc. could be good references for organisations to follow.

## *3.2 Evaluation (Methodology and Process)*

In order to feed the WCSC evaluation model, it is necessary to collect various data that implies workforce capability and response to security incidents, which is typically dependent on; ICS policy guidelines and operational objectives, workforce population size, evaluation timeline, and quality of expected feedback.

Data that represents WCSC is collected in a discrete format. The evaluation can be performed for an individual and/or an organisation. Data collection could be completed through 5 methodologies: *(i) Questionnaires, (ii) Interviews, (iii) Observations, (iv) Attack Simulations (Penetration Testing), and (v) Gamification.* These approaches can be employed individually or jointly. Data collection should meet the defined security evaluation requirements.

### 3.3 WCSC Evaluation Modelling

Here, the discrete data from the collection of responses are fed into a computational model as independent variables to obtain specific capability values. As *WCSC* is described as a function of the *Knowledge* and *Skills* of the workforce, represented in Eq. (1). A Capability Score Group is formulated to describe differing levels with respective score allocations. Table 1 provides the definition of each level of WCSC, and the WCSC score is evaluated from 5 to 1, implying from higher level to lower level.

$$WCSC = (Knowledge \times Skills) \tag{1}$$

**Mathematical Model** The set of WCSC scores, denoted as A = $\{x_1 \ldots x_5\}$, can be evaluated from the collection of feedbacks (directly or indirectly) from the selected workforce. This can be modelled as a set of algebraic function where set $A$; $x_1 \ldots x_5$ describes a set of values that define the variable score allocations. The function $f(x)$ describes a specific Cumulative Score ($CS$), and it is the product of $x$ and number of occurrence ($n_x$) in the feedback data. The *value* of $f(x)$ is formulated in Eq. (2). All possible values of $f(x)$ forms a set of B.

$$CS = f(x) = xn_x \tag{2}$$

*Following Table 1, Domain of A: {x |1 ≤ x ≤ 5}, Range of B: {f(x) = $xn_x$} (CS of each x in A; A = 1–5).*

An individual $p$ in the workforce could yield various occurrences of $x$ values. The sum of the cumulative scores of $x$ values is used to represent the WCSC of the individual p. Hence, the Quantitative Cumulative Score of the individual $p$, $Q_{csp}$, representing *knowledge* awareness or diagnostic s*kills, formulated as* Eq. (3).

**Table 1** Levels of WCSC

| Classification | Score (allocation) | Capability translation |
|---|---|---|
| Higher capability | 5 | Higher likelihood to respond desirably, and manage both indirect and targeted threats and cyber-attacks |
| High capability | 4 | High likelihood to respond desirably, and manage both indirect and targeted threats and cyber-attacks |
| Moderate capability | 3 | Moderate likelihood to respond desirably, and manage both indirect and targeted threats and cyber-attacks |
| Low capability | 2 | Low likelihood to respond desirably, and manage both indirect and targeted threats and cyber-attacks |
| Lower capability | 1 | Lower likelihood to respond desirably, and manage both indirect and targeted threats and cyber-attacks |

$$Q_{csp} = \sum_{i=1}^{5} f(x_i) \tag{3}$$

$\forall\ x_i \in x$, *and* $i = 1–5$; *in the domain of Cyber Security capability levels.*

The $Q_{csp}$, representing knowledge awareness of an individual p is denoted as $Ka_p$, and the $Q_{csp}$, representing the diagnostic skills, is denoted as $Sd_p$, A geometric mean offers the strengths of less submissiveness to the vast skewness influence of very large values in a range of distribution [25], and appropriateness for normalising the two quantities, such that neither quantity score alone perpetually dominates the weighting of the final result. Therefore, the *WCSC* score of an individual *p*, *CRp*, could be derived using a geometric mean—Eq. (4).

$$\begin{aligned} CR_p &= \sqrt{\left(f(x_i)_{p|Ka} \times f(x_i)_{p|Sd}\right)} \\ &= \sqrt{Ka_p \times Sd_p} \end{aligned} \tag{4}$$

With the $CR_p$ ratings of $n$ individuals, representing the workforce under evaluation, it becomes feasible to obtain a possible workforce capability of an entire organisation. This could be achieved by taking the Arithmetic Mean; *AM* of the set of $n$ individual capability scores—see Eq. (5). At the end, identification and categorisation of workforce capability is achieved using 3 fractional (grouped) ratios, 1:2:3. The motive is to map the workforce into disparate capability groups with unequal, successive priority ranges. *Capability table, scattered chart, and line graph*, are used to (re)present the derived discrete results into quick human comprehensible format.

$$OWCC = \frac{\sum_{p=1}^{n} \left(\sqrt{Ka_P \times Sd_P}\right)}{n} \tag{5}$$

## 4 Theoretical Validation

An initial conjectural test of the WCSC evaluation model is presented using a virtual test data to observe model behaviour, and examine its suitability for the context of the study. This hypothetical validation approach is adopted for quick valuation of the behaviour of the model relative to an expected behaviour, and also due to non-availability of real analytical data about individual responses of a target industrial workforce (*implying IT security experts, engineers, field operators, technicians, and corporate users*) under evaluation. Acquiring such primary data from organisations is pretty difficult. Most organisations are unwilling to disclose security capability details of their employees, which in most cases often unveil to external parties; personnel the cyber security weaknesses, and the vulnerabilities of systems they operate. Organisations are always scared and apprehensive to provide

third parties with lead-ins to utilize the data of their employees. Nobody is willing to take the risks of having such intellectual details in wrong hands capable of engineering exploitation for competitive advantage or outright sabotage. However, if meaningful results could be derived by testing the model on the virtual data, then the model could be applicable to real data, which could have similar pattern with the virtual cases.

## 4.1 Basic Assumptions

Assume that some prior stages (*Steps 1.1, 1.2, 1.3, and 2.1*) of the evaluation process-flow have been accomplished. The receipt of real response/feedback data about the Cyber security capability of an arbitrary industrial workforce is also presumed. Other assumptions employed to help meet the conditions of this typical capability data aggregation procedure include: outline of organisation-specific cyber security requirements, selection of target industrial workforce with initial sample size of 50, a questionnaire with two sets of 15 questions for awareness and skills respectively, each question has 5 multiple options with score allocations in Table 1, initial aggregation and computation of workforce capability ratings for knowledge and skills is accomplished in line with Eq. (4*)* above.

## 4.2 Data Generation and Priority Classification (Benchmarks)

Following the above assumptions, a random data function in *Matlab* is used to generate values for the independent variables in the mathematical model. Accordingly, dependent variables values, WCSC ranking, and the range of each level are presented in Table 2, with scattered charts for visualising the positions of the WCSC score shown in Fig. 3.

## 4.3 Results and Discussions

The WCSC ranking of $n = 50$ randomly generated pairs of vector values, representing the $Q_{csp}$ in Knowledge ($Ka_p$), *and Skills* ($Sd_p$) respectively; is based on the WCSC score, which is the geometric mean of $Ka_p$ and $Sd_p$ (Eq. 4). For instance,

**Table 2** WCSC ranking

| Level of WCSC | Ratio (upper limit) | Priority range |
|---|---|---|
| High (*h*) | 1/3 | $15 \leq h \leq 25$ |
| Moderate (*m*) | 2/3 | $25 < m \leq 50$ |
| Low (*l*) | 3/3 | $50 < l \leq 75$ |

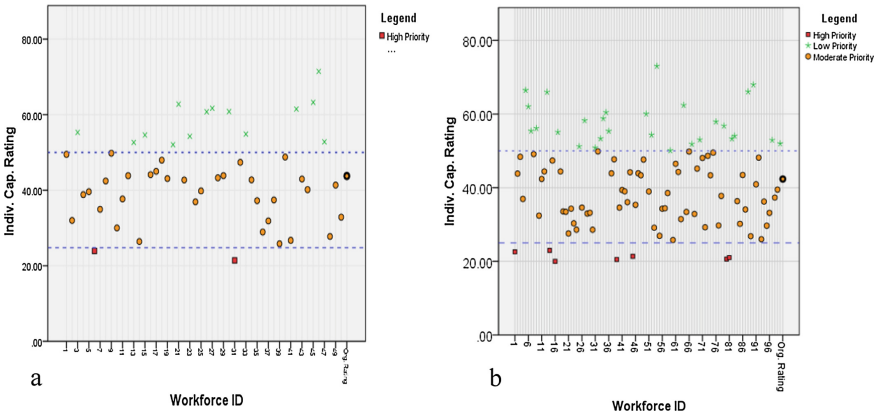


**Fig. 3** Workforce cyber security capability visualization chart. **a** 50 Users, **b** 100 Users

$Ka_p$ = 29, and $Sd_p$ = 63, yields a WCSC score of the individual $CR_p \cong 42.74$, which falls within a '*moderate level*'. Regardless whether the examined entity had a '*moderate level*' knowledge or a '*low level*' skills, the overall WCSC score is scaled down to '*moderate*'. Another example, $Ka_p$ = 71, and $Sd_p$ = 20, resulting in $CR_p \cong 37.68$.

Based on the WCSC ranking, 14 workforce members have '*Low level*' of WCSC. 34 workforce members have '*Moderate level*' of WCSC, while 2 member workforce yielded '*High leve*l' of WCSC (see Fig. 3a). The organisational WCSC is about 43.76, falling within the '*Moderate level*' of WCSC ranking, and it has a standard deviation (*std*) of 11.75. The standard deviation, which describes the capability dispersion of the workforce relative to the average capability, illustrate some measures of capability gaps.

The process repeated for n = 100 sample workforce, and the results show 28 '*Low level*' of WCSC, 65 '*Moderate level*' of WCSC, and 7 '*High level*' of WCSC (see Fig. 3b). Organizational WCSC is about 42.35, with *std* ≅ 12.38.

Generally, results suggest that regardless of the number of high-skilled IT security workforce members in an industrial environment, the presence of other OT workforce members with low WCSC could reduce overall organisational WCSC. Contextually, it supports that the workforce members with low WCSC level are the weak-links and more prominent targets of attacks. Metaphorically, with a strawed portion in a brick wall, the wall becomes more vulnerable. Results also indicate that a low capability of either knowledge or skills directly affects the overall WCSC. A lack or low capability of both is worse still. Essentially, a workforce entity that is abreast with knowledge in the emerging industrial Cyber security landscape, but lacking the practical (responsive) skills and expertise to ensure security within his/her domain, is as weak as the one who is skilled in managing and responding to primordial cyber security threats and attacks, but does not continually keep-up with updates in information and details on the changing security landscape. This

scenario represents a potential normal situation within an organisational domain, where little emphasis is placed on cyber security assurance.

Based on observed results, it is suggested that the reduction or increase of mean organisational WCSC depends on the application of potential remediation schemes or control measures. Probable increase in organisational WCSC could be typically explained as the outcome of the broad increase in individual workforce capabilities.

While introducing an individual to an organisation, his/her WCSC more or less affects the organisational WCSC by introducing either a positive or a negative weight on the current organizational WCSC. Practically, the individual WCSC might introduce an intersecting effect that potentially widens already existing weaknesses, thus dropping overall organisational WCSC. Under this circumstances, it is projected that the mean WCSC will continue to decrease, because the mean emerges as a results of the introduction of lower capability values. However, if the requisite capability building and enhancement activities are identified and initiated, positive weights could be exerted on the current organizational capability. A potential improvement of WCSC, could be achieved; as more regular interactions amongst the workforce allow them to share and improve the security awareness and skills.

In the course of engaging remediation strategies, the knowledge from such evaluation would enable organisations to identify those individuals who need to be trained for the improvement of WCSC, and help organisations adopt a cost-effective means of narrowing and appropriating remediation schemes, scopes, and resources without waste or excessive spending. The opposite is usually the engagement of all-purpose remediation after surveys and evaluations that yield outcomes, but with uncertainties in capability levels and attributions about the industrial workforce.

## 5 Conclusion and Future Work

In the modern computing insecurity era, where the human workforce has become prime vectors and targets of successful industrial cyber incidents, understanding the cyber security knowledge, and skills capabilities of the industrial personnel is key to developing a more effective and skilled cyber workforce. Great deal of records show that most successes in the malicious compromise of industrial networks and systems have rested on the exploitation of weakness or vulnerabilities from the workforce with low WCSC. Targeted attacks on the workforce become successful for one of two reasons; workforce inappropriate or improper behaviour due to lack of knowledge, skills enough to counteract malicious actions. The application of strategic and systematic study and analysis can spur the industry towards good cyber hygiene, and help sustain efficient response to the necessary cyber security factors, and thus reduce to the barest minimum; weak links in the system.

This paper addressed the importance of WCSC evaluation, which, is a means of spurring organisations to improve their workforce cyber security assurance. Having a WCSC evaluation could help organisations to identify specific cyber security

threats and vulnerabilities, where security need to be improved, and help organisations to setup prospective WCSC, in comparison to benchmarked cyber-attacks.

In general, the WCSC model could offer a starting point for managers or security auditors to examine the respective postures of their workforce in terms of Cyber security objectives. Correspondingly, the overall organisational WCSC is a means of measuring the effectiveness of continuous cyber security efforts, and speed-up problem-solving. Organisationally, WCSC evaluation model could also help the regulation of resource application, tailor remediation, capacity building needs to meet, changing and future capability trends, cyber security assurance measures, and fundamental modifications in the way assurance is achieved.

Future works include; developing an evaluation tool that could integrate seamlessly with the proposed framework, and validate the model with real industrial data. Work will be done on developing ICS-specific cyber security metrics, and formulation of a risk-based solution for enhancing cyber security assurance.

## References


1. Bayuk, J.L., Healey, J., Rohmeyer, P., Sachs, M.H., Schmidt, J., Weiss, J.: Cyber Security Policy Guidebook. Wiley, Hoboken, New Jersey (2012)
2. Goutam, R.K.: Importance of Cyber Security. Int. J. Comput. Appl. (0975–8887), **111**(7), 8887 (2015)
3. King-Turner, M.: Three Keys to IT System Success: People, Process, Technology (National B2B Centre). The National B2B Centre, UK (2014). [Online]. Available: http://www.nb2bc.co.uk/managing_it_projects/articles/?id=181. Accessed 12 Aug 2015
4. Ramakrishnan, S., Testani, M.: People, Process, Technology—The Three Elements for a Successful Organizational Transformation. IBM Path Forward to Business Transformation. IBM Centre for Learning and Development, pp. 1–21 (2011)
5. Howarth, F.: The Role of Human Error in Successful Security Attacks. Security Intelligence Website. IBM Security Intelligence (2014)
6. Gonzalez, C., Ben-Asher, N., Oltramari, A., Lebiere, C.: Cognition and technology. In: Cyber Defense and Situational Awareness, pp. 93–117 (2014)
7. Chen, P.-C., Liu, P., Yen, J., Mullen, T.: Experience-based cyber situation recognition using relaxable logic patterns. IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support **2012**, 243–250 (2012)
8. Ben-Asher, N., Gonzalez, C.: Effects of cyber security knowledge on attack detection. Comput. Human Behav. **48**, 51–61 (2015)
9. IRM: "Amateyrs attack technology. Professional hackers target people. Website Article, 2015. [Online]. Available: https://www.irmplc.com/issues/human-behaviour/. Accessed 15 Jun 2015
10. Navarro, L.: Train employees—your best defense—for security awareness. SC Magazine Online (2007)
11. Russell, C.: Security Awareness—Implementing an Effective Strategy (2002)
12. Kaspersky-Labs: Kaspersky Lab: Empowering Industrial Cyber Security (2015)
13. Robert, H.: Humans 'often the weakest link' when it comes to cyber security. NCC Group Website: New Room, 2015. [Online]. Available: https://www.nccgroup.trust/uk/about-us/newsroom-and-events/news/2015/july/humans-often-the-weakest-link-when-it-comes-to-cyber-security/. Accessed 10 Sept 2015

14. Wombat: Wombat Security Technologies Unveils CyberStrength, a First of its Kind Security Awareness Assessment Solution that Helps Companies Measure Employee Vulnerability to Cyber Security Attacks—Wombat. Website Article, 2013. [Online]. Available: https://www.wombatsecurity.com/press-releases/wombat-security-technologies-unveils-cyberstrength-first-its-kind-security-awareness. Accessed: 14 Aug 2015
15. Debo, C.: Preventing Cyberattacks and Data Breaches via Employee Awareness Training and Phishing Simulations. Website Article, 2015. [Online]. Available: http://www.schneiderdowns.com/preventing-cyberattacks-data-breaches-employee-awareness-training-phishing-simulations. Accessed: 14 July 2015
16. Zurko, M.E.: User-centered security: Stepping up to the grand challenge. Proceedings—Annual Computer Security Applications Conference, ACSAC **2005**, 187–200 (2005)
17. Johnson, T.A.: Cyber Security: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare. CRC Press, Taylor & Francis Group, Boca Raton (2015)
18. ITU: 2013 ITU survey on measures taken to raise awareness on Cyber Security, Aug 2013, pp. 1–27 (2013)
19. Toth, P., Klein, P.: A Role-Based Model for Federal Information Technology/Cyber Security Training (2014)
20. D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., Roth, E.: Achieving cyber defense situational awareness: a cognitive task analysis of information assurance analysts. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 2005, vol. 49, pp. 229–233
21. Botta, D., Werlinger, R., Gagné, A., Beznosov, K., Iverson, L., Fels, S., Fisher, B.: Towards understanding IT security professionals and their tools. In: SOUPS '07: Proceedings of the 3rd Symposium on Usable Privacy and Security, 2007, pp. 100–111
22. Paul, C.L., Whitley, K.: A taxonomy of cyber awareness questions for the user-centered design of cyber situation awareness. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 8030 LNCS, pp. 145–154 (2013)
23. Aloul,F.A.: The need for effective information security awareness. J. Adv. Inf. Technol. **3**(3), 176–183 (2012)
24. Parsons, K., Mccormac, A., Butavicius, M., Ferguson, L.: Human Factors and Information Security : Individual, Culture and Security Environment. Edinburgh South Australia (2010)
25. Manikandan, S.: Measures of central tendency: the mean. J. Pharmacol. Pharmacother. **2**(2), 140 (2011)

2016-07-10

# Human capability evaluation approach for cybersecurity in critical industrial infrastructure

Ani, Uchenna P.

Springer

Ani, U. P., He, H., Tiwari, A. (2016) Human capability evaluation approach for cybersecurity in critical industrial infrastructure, Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2016 International Conference on Human Factors in Cybersecurity, July 27-31, 2016, Walt Disney World, Florida, USA, Part III, pp. 169-182

http://dx.doi.org/10.1007/978-3-319-41932-9_14